

Please REPLACE the paragraph beginning at page 40, line 9, as follows:

FIGURE 33A shows an example of the first type of encryption device 100 shown in FIGURE 21, which is an encryption device 700 in accordance with the DES encryption of FIGURES 32A and 32B to which the fixed mask value method is applied in a manner similar to the encryption device 400 of FIGURE 29. FIGURE 33B shows a more detailed configuration of a F function shown in FIGURE 33A. In FIGURE 33A, the processor 150, the memories 160, 162 and 164 shown in FIGURE 21 are not shown for simplicity.

Please REPLACE the paragraph beginning at page 41, line ¹⁴~~18~~, as follows:

5/18

The processor 150 in FIGURE 21 controls the processing elements 701 to 763 and the like of the encryption device 700 of FIGURES 33A and 33B in accordance with the program stored in the program memory 160. Alternatively, the processor 150 may provide the processing elements 701 to 763 and the like, by executing the program in the memory 160 which is implemented to provide the functions corresponding to the processing elements 701 to 763 and the like. In this case, FIGURES 33A and 33B may be considered as a flow diagram.

Please REPLACE the paragraph beginning at page 41, line 26, as follows:

FIGURE 34A shows an example of the second type of encryption device 200 shown in FIGURE 24, which is an encryption device 800 in accordance with the DES encryption of FIGURES 32A and 32B to which the fixed mask value method is applied in a manner similar to the encryption device 500 of FIGURE 31. FIGURE 34B shows a more detailed configuration of a F function shown in FIGURE 34A. In FIGURE 34A, the processor 250, the memory 260, 262 and 264 shown in FIGURE 24 are not shown for simplicity.

Please REPLACE the paragraph beginning at page 42, line 5, as follows:

The processor 250 in FIGURE 24 controls the processing elements 801 to 862 and the like of the encryption device 800 of FIGURES 34A and 34B in accordance with the program stored in the memory 260. Alternatively, the processor 150 may provide the processing elements 801 to 862 and the like, by executing the program in the memory 160 which is implemented to provide the functions corresponding to the processing elements 801 to 862 and the like. In this case, FIGURES 34A and 34B may be considered as a flow diagram.

IN THE SPECIFICATION:

The specification as amended below with replacement paragraphs shows added text with underlining and deleted text with ~~strikethrough~~.

Please REPLACE the paragraph at page 38, lines ¹⁻⁴~~1-5~~, with the following paragraph: *yes/18*

TABLE 2. Relation between Mask Value and Amount of Computation Required for Determining 128-bit Secret Key by DPA of Loading Sbox ~~Output-Input~~ Values, for One Common Sbox Set for Subbytes, in Fixed Mask Value Method.

Please REPLACE the paragraph at page 41, lines 1-15, with the following paragraph:

The F function of FIGURE 33B includes a selector 759 for providing a fixed mask value $FM_{i,h}$ selected in response to the random number h , an XOR 762 for XORing the sub-key K_i with the fixed mask value $FM_{i,h}$ to provide an output, an XOR 763 for XORing the output value with an input X_i' linearly transformed by a linear transform E , selectors 752 to 756 for selecting one of Subbytes $[[S_{i,h}]] \underline{S_{i,h}}$ in response to the random number h to provide the output from the XOR 763, Subbytes $[[S_{i,h}]] \underline{S_{i,h}}$ for performing the Subbyte in accordance with the respective nonlinear table Sboxes $[[S_{i,h}]] \underline{S_{i,h}}$, selectors 754 to 757 for selecting one of the Subbytes $[[S_{i,h}]] \underline{S_{i,h}}$ in response to the random number h to provide an output, and a linear transform P for linearly transforming the output from the selectors 754 to 757 to provide an output Z_i' .

Please REPLACE the paragraph at page 42, lines 24-30, with the following paragraph:

The F function of FIGURE 34B includes an XOR 862 for XORing the input X_i' linearly transformed by a linear transform E with the XOR value of the sub-key K_i with the fixed mask value $FM_{i,h}$, Subbytes $[[S_{i,h}]] \underline{S_{i,h}}$ ($i = 1, 2, \dots, 8$) in accordance with the nonlinear table SBoxes $S_{i,h}$, and a linear transform P for linearly transforming the output from the Subbyte $[[S_{i,h}]] \underline{S_{i,h}}$ to provide an output Z_i' .